IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Kevin Fu et al.	§	Art Unit:	2131
Serial No.:	10/624,403	§		
		§	Examiner:	Shin Hon Chen
Filed:	July 21, 2003	§		
For:	Windowed Backward Key Rotation	§	Atty. Dkt. No.:	200311171-1 (HPC.0593US)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-21 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

Date of Deposit: November 03, 2008

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent Office on the date indicated above.

Ginger Yount

II. RELATED APPEALS AND INTERFERENCES

The following is a related appeal: Appeal Brief filed on August 6, 2007, in U.S. Serial No. 10/355,470 (now U.S. Patent No. 7,313,238). The inventors of the '470 application are Kevin E. Fu, Mahesh Kallahalla, and Ram Swaminathan. The Assignee of the '470 application is the Hewlett-Packard Development Company, L.P. The legal representative that submitted the Appeal Brief in the '470 application is Dan C. Hu, Registration No. 40,025.

The '470 application was identified as a related application on page 1 of the present Specification. In response to the Appeal Brief filed on August 6, 2007 in the '470 application, a Notice of Allowance was mailed on October 29, 2007.

III. STATUS OF THE CLAIMS

Claims 1-21 have been finally rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendments after final rejection have been submitted.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a method of windowed backward key generation, comprising:

a) providing (Fig. 4:420) information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series and wherein said information is derived from at least one of said limited number of previous key in said series (Spec., p. 19, lines 1-8; p. 15, line 10-page 16, line 7);

b) generating (Fig. 4:440) a key in the series, based at least in part on said information provided to said user (Spec., p. 19, lines 16-19);

c) providing (Fig. 4:450) said key in the series to the user (Spec., p. 19, lines 21-22); and

d) said user determining (Fig. 4:480) at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user (Spec., p. 20, line 21-p. 21, line 2).

Independent claim 8 recites a method of windowed backward key rotation, comprising:

a) providing (Fig. 4:420) to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable by the user but previous versions of the key rotation element are not determinable by said user (Spec., p. 19, lines 1-8; p. 15, line 10-p. 16, line 7);

b) generating (Fig. 4:440) a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer (Spec., p. 19, lines 16-19);

c) providing (Fig. 4:450) to the user the later version of the key (K_{i+n}) (Spec., p. 19, lines 21-22); and

d) said user determining (Fig. 4:480) a version of the key from (K_i-K_{i+n-1}), inclusive, by applying a version of the key rotation element to a version of the key from (K_{i+1}-K_{i+n}), inclusive (Spec., p. 20, lines 21-22).

Independent claim 15 recites a method of windowed backward file key generation, comprising:

a) generating (Fig. 4:410) an initial file key (Spec., p. 19, lines 4-5);

b) generating (Fig. 4:410) an initial key rotation exponent, wherein said initial key rotation exponent allows previous versions of the file keys to be determined back until a pre-determined version of the file key, but no file keys further back (Spec., p. 19, lines 4-5; p. 20, lines 4-20); and

c) providing (Fig. 4:420) said initial file key and said initial key rotation exponent to initial users (Spec., p. 19, lines 7-8).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 2, 4-6, 8-13, and 15-21 Rejected Under 35 U.S.C. § 102(a) as Anticipated by U.S. Patent Application Publication No. 2002/0152392 (Hardy).

B. Claims 3, 7, and 14 Rejected Under 35 U.S.C. § 103(a) as Unpatentable Over Hardy Alone.

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1, 2, 4-6, 8-13, and 15-21 Rejected Under 35 U.S.C. § 102(a) as Anticipated by U.S. Patent Application Publication No. 2002/0152392 (Hardy).

1. Claims 1, 2, 4-6.

Independent claim 1 was erroneously rejected as being anticipated by Hardy.

Claim 1 recites a method of windowed backward key generation, comprising:

a) providing information to a user that allows **determining a limited number of previous keys in a series of keys from a later key** in the series and wherein said information is derived from at least one of said limited number of previous key in said series;

b) generating a key in the series, based at least in part on said information provided to said user;

c) providing said key in the series to the user; and

d) said user determining at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user.

Hardy does not teach providing information to a user that allows determining a limited number of **previous** keys in a series of keys **from** a **later** key in the series. In Hardy, for each previous, or subsequent, version of a software product being accessed by a user, a unique key is generated which is **independent** of any other keys used to decrypt the software product.

As taught by Hardy, an initial software product is encrypted using KEY A, which is generated by a random number generator. Hardy, ¶ [0015]. If the initial software product is changed such that a different version of the software product is provided, then Hardy teaches that the different version of the software product is encrypted with a new encryption key, KEY B, which is generated by a random number generator. *Id.*, ¶ [0021].

There is absolutely nothing in Hardy that even remotely hints that KEY A can be determined from KEY B. Note that claim 1 specifically states that information is provided to a user that allows determining a limited number of **previous keys** in series of keys from a **later key** in the series. If KEY B is considered the later key of claim 1, then there is absolutely no teaching whatsoever in Hardy that KEY A can be determined from KEY B.

The Response to Arguments section of the 6/6/2008 Office Action states that KEY B is not found in the claim, and therefore, the Examiner did not have to address Appellant's arguments made in the previous Reply to Office Action. 6/6/2008 Office Action at 5. However, the Examiner has failed to identify what in Hardy constitutes the following element of claim 1: providing information to a user that allows determining a limited number of **previous keys** in a

series of keys from a **later key** in the series. With respect to this clause, the Examiner appears to have referred to ¶¶ [0007] and [0021] of Hardy generally, without identifying what in Hardy specifically constitutes the later key and the previous keys, and how such previous keys can be determined from the later key. It is apparent that the Examiner can find nothing in Hardy that corresponds to the above claim feature.

The Examiner also refers to the SPLIT information that is provided to a user in Hardy; note, however, that the SPLIT information of Hardy is a decryption code that is provided to a user for combination with a token (TOKEN) to derive KEY A; however, this does not rise to the level of determining a previous key from a later key, as recited in claim 1.

Since Hardy clearly fails to provide any teaching or hint of the claimed subject matter, the rejection of claim 1 and its dependent claims over Hardy is clearly erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 8-13.

Independent claim 8 was also erroneously rejected as being anticipated by Hardy. Claim 8 recites a method of windowed backward key rotation, comprising:

> a) providing to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable by the user but previous versions of the key rotation element are not determinable by said user;
>
> b) generating a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer;
>
> c) providing to the user the later version of the key (K_{i+n}); and
>
> d) said user determining a version of the key from (K_i-K_{i+n-1}), inclusive, by applying a version of the key rotation element to a version of the key from (K_{i+1}-K_{i+n}), inclusive.

As recited in claim 8, one version of a key from (K_i-K_{i+n-1}), inclusive, is determined another version of the key from (K_{i+1}-K_{i+n}), inclusive. As explained above in connection with claim 1, Hardy provides absolutely no teaching whatsoever of determining one version of a key from another version of the key. As taught by Hardy, random number generators are used to independently generate unique keys for different versions of a software product.

In view of the foregoing, claim 8 and its dependent claims are clearly not anticipated by Hardy.

Reversal of the final rejection of the above claims is respectfully requested.

3. Claims 15-17, 19-21.

Independent claim 15 is also not anticipated by Hardy. Claim 15 recites an initial key rotation exponent that allows previous versions of file keys to be determined back until a pre-determined version of the file key, but not file keys further back. Note that one initial key rotation exponent allows multiple previous versions of file keys to be determined.

If SPLIT in Hardy is considered to be the key rotation exponent of claim 15, then SPLIT cannot be used to determine multiple previous versions of file keys, as recited in claim 15; in Hardy, SPLIT A would be used to determine just the current key, KEY A. Therefore, claim 15 and its dependent claims are clearly not anticipated by Hardy.

Reversal of the final rejection of the above claims is respectfully requested.

4. Claim 18.

Claim 18 depends from claim 15, and is therefore allowable for at least the same reasons as claim 15. Moreover, claim 18 recites a user generating a previous version of the file key by applying a version of the key rotation exponent to a version of the file key. Note that Hardy does

not contemplate at all generating one version of the file key from another version of the file key; in Hardy, random numbers are generated by random number generators to produce respective unique keys for different versions of software.

Therefore, claim 18 is further allowable for the foregoing reason.

Reversal of the final rejection of the above claim is respectfully requested.

B. Claims 3, 7, and 14 Rejected Under 35 U.S.C. § 103(a) as Unpatentable Over Hardy Alone.

1. Claim 3.

In view of the defective rejection of base claim 1 over Hardy, the obviousness of rejection of claim 3 over Hardy alone is defective.

Moreover, claim 3 further recites providing to the user a key rotation exponent that is used to determine a previous key in the series from a later key in the series by exponentiating the later key by the key rotation exponent.

The Examiner argued that it would have been obvious to one of ordinary skill to utilize exponentiation "in place of the logical addition ...." 6/6/2008 Office Action at 4. However, as explained above, Hardy discloses using random number generators to generate random numbers for corresponding unique keys for different versions of software; there is absolutely no teaching whatsoever in Hardy of generating one key from another key. Even more specifically, Hardy provides absolutely no hint of determining a previous key in the series from a later key in the series by exponentiating the later key by the key rotation exponent. Except for the claim itself, the Examiner has identified no objective evidence that would have prompted a person of ordinary skill in the art to modify the teachings of Hardy to achieve the claimed subject matter. Therefore, the obviousness rejection of claim 3 is clearly defective.

Reversal of the final rejection of the above claim is respectfully requested.

2. Claims 7, 14.

In view of the defective rejection of base claims 1 and 8 over Hardy, the obviousness rejection of dependent claims 7 and 14 over Hardy is also defective. Moreover, claim 7 further recites that a user is revoked by publishing a version of the revoked user's secret share. The Examiner provided a conclusory statement that this feature of claim 7 would be obvious to a person of ordinary skill in the art, without providing any basis in fact. In the rejection of claim 5 (from which claim 7 depends), the Examiner identified TOKEN and SPLIT as constituting the secret share and key rotation catalyst. 6/6/2008 Office Action at 3. However, there is absolutely no teaching or hint given by Hardy that publishing TOKEN or SPLIT would cause revocation of a user. Therefore, the obviousness rejection of claim 7 is clearly defective.

Claim 14 is similarly allowable over Hardy.

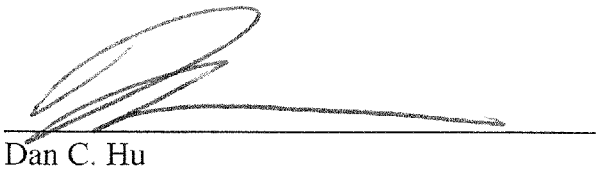
Reversal of the final rejection of the above claims is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: Nov 3, 2008



Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1. A method of windowed backward key generation, comprising:

a) providing information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series and wherein said information is derived from at least one of said limited number of previous key in said series;

b) generating a key in the series, based at least in part on said information provided to said user;

c) providing said key in the series to the user; and

d) said user determining at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user.

2. The method of Claim 1, wherein said a) comprises providing a key rotation element that is forward rotatable by said user but is not backward rotatable.

3. The method of Claim 1, wherein said a) comprises providing to the user a key rotation exponent that is used to determine a previous key in the series from a later key in the series by exponentiating said later key by said key rotation exponent.

4. The method of Claim 2, further comprising:

e1) generating a new key rotation element;

e2) generating a new key based, in part, on said new key rotation element; and

e3) distributing said new key to non-revoked users.

5. The method of Claim 1, wherein said a) further comprises providing a secret share and a key rotation catalyst to said user, wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available.

6. The method of Claim 5, further comprising:

e) publishing at least one public share, wherein the next key in the series is determinable based on the key rotation catalyst, the secret share, and the at least one public share.

7. The method of Claim 5, further comprising revoking a user by publishing a version of the revoked user's secret share.

8. A method of windowed backward key rotation, comprising:

a) providing to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable by the user but previous versions of the key rotation element are not determinable by said user;

b) generating a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer;

c) providing to the user the later version of the key (K_{i+n}); and

d) said user determining a version of the key from (K_i-K_{i+n-1}), inclusive, by applying a version of the key rotation element to a version of the key from (K_{i+1}-K_{i+n}), inclusive.

9. The method of Claim 8, wherein said d) comprises:

d1) said user determining a later version of said key rotation element from said key rotation element provided in said a).

10. The method of Claim 9, wherein said d) further comprises:

d2) said user determining the version of the key K_{i+n-1} by applying the version of the key rotation element to the version of the key K_{i+n}.

11. The method of Claim 8, further comprising:

e1) generating a new key rotation element;

e2) generating a new key based, in part, on said new key rotation element; and

e3) distributing said key to non-revoked users.

12. The method of Claim 8, wherein said a) further comprises providing a secret share and a key rotation catalyst to said user, wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available.

13. The method of Claim 12, further comprising:

e) publishing at least one public share, wherein the next key in the series is determinable based on the key rotation catalyst, the secret share, and the at least one public share.

14. The method of Claim 12, further comprising revoking a user by publishing a version of the revoked user's secret share.

15. A method of windowed backward file key generation, comprising:

a) generating an initial file key;

b) generating an initial key rotation exponent, wherein said initial key rotation exponent allows previous versions of the file keys to be determined back until a pre-determined version of the file key, but no file keys further back; and

c) providing said initial file key and said initial key rotation exponent to initial users.

16. The method of Claim 15, further comprising:

d) joining a new user by distributing said new file key and said new key rotation exponent to said user.

17. The method of Claim 15, further comprising:

d1) generating a new key rotation exponent;

d2) generating a new file key based, in part, on said new key rotation exponent; and

d3) distributing said new file key to non-revoked users.

18. The method of Claim 15, further comprising:

d) a user generating a previous version of the file key by applying a version of the key rotation exponent to a version of the file key.

19. The method of Claim 15, wherein:

said a) further comprises generating a key rotation catalyst; and

said c) further comprises providing a secret share and said key rotation catalyst to ones of said initial users, wherein said secret share and said key rotation catalyst allow said initial users to generate a new version of the file key provided sufficient public information is available.

20. The method of Claim 19, further comprising:

d) publishing a public share, wherein said initial users are able to determine a new version of the file key using their own secret shares, the public shares, the key rotation catalyst, and a previous file key.

21. The method of Claim 19, further comprising:

d1) generating a new key rotation catalyst;

d2) publishing said new key rotation catalyst;

d3) generating a new file key based, in part, on said new key rotation catalyst; and

d4) publishing a revoked user's private share.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.